# U.S. Comprehensive Consumer Privacy Laws Frequently Asked Questions

The patchwork of over 19 states with differing consumer privacy laws has created compliance challenges for businesses across the country – and they often stem from the fact that businesses are justifiably confused about some of these laws' basic principles. This series of Frequently Asked Questions, prepared by the Fisher Phillips' Consumer Privacy Team, offers a thorough resource to help not only those brand new to these state laws, but also those well-versed and experienced in compliance efforts. The information here is a general overview and may not be specific to a particular state. Please contact a Fisher Phillips Consumer Privacy Team attorney to obtain specific, appropriate legal advice.

**1. If my business doesn't have a presence in any of the states that have a comprehensive consumer privacy law, do I have to comply with any of these laws?**

Potentially, yes, if you meet one of the threshold criteria for applicability. Even if you are not organized under that state's law and have no physical presence in the state, you may be subject to that state's comprehensive consumer privacy law. If you do business with residents of the state either in person, over the phone, or through a website, these laws may apply to your business.

**2. Who is a consumer?**

A consumer is a natural person who is a resident of the state, as defined in the state's regulations, however identified, including by any unique identifier. For most states this is where the definition ends. In California however, and despite the word choice, a consumer also includes other categories of individuals including job applicants, current and former employees, emergency contacts, dependents and beneficiaries, board members, members of an organization, temporary workers, independent contractors, and others, if they are a California resident.

Physical presence in a state does not automatically qualify the consumer as a resident of the state, and the law does not create a presumption of residency status based solely on the interaction taking place in a particular state. There are several varying tests for residency status under these state laws.

**3. Which of these comprehensive consumer privacy laws is my business subject to, if any?**

All of the state comprehensive consumer privacy laws have a threshold for applicability based on a number of differing factors often requiring:

A minimum gross revenue

A minimum number of state residents or households whose personal information a business controls, collects, processes, buys, sells, or shares,

or

A minimum annual revenue percentage that the business received from buying, selling, or sharing consumer personal information.

Another way your business could be subject to the law relates to whether your business controls or is controlled by a CCPA-covered business while also sharing common branding and sharing personal information. Or you could operate a joint venture or partnership in which any covered business has at least a 40% interest.

**4. Are the revenue thresholds just for revenue generated in that state?**

No. The revenue threshold is established by gross revenue regardless of source, location of where the revenue is generated, or any other factor. Thus, all gross revenue from anywhere in the world should count towards the threshold, not just that particular state's revenue.

**5. Over what period is revenue measured?**

Revenue is typically calculated based on all revenue generated during the prior calendar year (that is, from January 1 through December 31). That means that as of January 1 in any given year, if the business did not meet the revenue threshold in the prior calendar year, then the next time the law may begin to apply to the business is the following January 1.

**6. What does it mean to "do business" in a state?**

Unfortunately, not all of the laws specify what this critical phrase means. A company might be considered to "do business" in a state even if it merely operates a website or app through which residents provide their personal information. The CCPA carves out a narrow exception if every aspect of commercial conduct takes place wholly outside of California.

The following is a non-exhaustive list of what may potentially constitute doing business in a state:

- Engaging in any transaction for the purpose of financial gain within the state
- Being domiciled in or maintaining a physical location
- Having one or more employees or independent contractors in the state
- Recruiting potential job applicants from the state
- Marketing or selling products or services in the state

**7. Will collecting data through our website count towards the "buy, sell, or share" criteria?**

Yes. Collection of a resident's data through a website can satisfy the initial requirement for applicability of the statute. This includes IP addresses and other internet activity information such as device ID, browser ID, what the user clicked on, etc. It remains unclear if the collection of data about website visitors through cookies and pixels and then sharing or selling this data would bring a business within the scope of this criteria.

**8. If we operate a franchisee, subsidiary, or parent company, how do we know if a statute applies to us?**

Even if you are not a covered business in some states, entities that control *or* are controlled by a covered business, along with those that share common branding with a covered business, can be covered by the law. This can include a shared name, servicemark, or trademark through which the average consumer would understand that two or more entities are commonly owned. In such cases, your business may not be exempt merely by being a franchisee or subsidiary.

**9. Are there any exceptions to the state comprehensive consumer privacy laws?**

Yes, depending on the state, there may be exceptions for businesses subject to other federal privacy laws such as the Gramm-Leach-Bliley Act (financial services companies) or those entities that are subject to HIPAA (Health Insurance Portability and Accountability Act). However, the exceptions are not absolute and may sometimes only apply to a part of your business. Exceptions are a difficult area of the consumer privacy laws; you should not assume that you have no obligations under state consumer privacy laws just because your business is subject to one of these federal privacy laws.

**10. How long do I have to comply with these state laws?**

Each state law has its own effective date, and generally they are effective as of that date. The latest state law to go into effect was Montana, on October 1, 2024. Click here for a list of the states with Comprehensive Consumer Privacy laws and the date the law went into effect.

**11. When will states begin enforcing requirements?**

Each state has its own enforcement agencies and typically states can begin enforcement upon the effective date of the law.

**12. What are the consequences for non-compliance? Are there enforcement penalties?**

Many of the state consumer privacy laws, provide specific penalties for violations. The state agency charged with enforcement would have the authority to enforce any penalty for violations that they impose.

Some state laws have a range of fines, or civil penalties, and the states each have varying monetary amounts for the fines. Generally, the fines range from $2,500 to $20,000 per violation of the statute. Civil penalties can only be imposed in enforcement actions by the State agency charged with the enforcement of the law.

In California, under the CCPA, the consequences for a data breach involving certain sensitive personal information are severe. This is in large part due to the CCPA's "private right of action" allowing California residents who prove a violation to recover statutory damages between $100 and $750 *per person*, *per incident*, even if the person cannot prove actual harm. These penalties can add up quickly, particularly in a class action context. Your defense against any statutory damages is being able to demonstrate that you implemented and maintained reasonable security procedures and practices.

**13. Do state comprehensive consumer privacy laws mean that people can file a lawsuit against my business?**

With the exception of California, none of the state laws in effect have a private right of action. This means that consumers can't bring a claim against a business for violation of the law. Only the state regulatory authorities, such as an agency or the state attorney general, can bring an action for failing to comply with the law. However, consumers can bring claims for privacy issues under other statutes or under a common law claim.

**14. What is the significance of the CCPA "private right of action"?**

Under the CCPA, individuals have a "private right of action," meaning that they can file a lawsuit against a business if certain categories of their nonencrypted and unredacted sensitive personal information was stolen in a data breach resulting from the business's failure to maintain reasonable security procedures and practices.

Currently, the CCPA limits a data breach to only unauthorized access and exfiltration, theft, or disclosure of an individual's first name or first initial and the individual's last name in combination with any one or more of the following data elements, when either the name or the data elements are not encrypted or redacted:

- Social security number
- Driver's license number, California identification card number, tax identification number, passport number, military identification number, or other unique identification number issued on a government document commonly used to verify the identity of a specific individual
- Account number or credit or debit card number, in combination with any required security code, access code, or password that would permit access to an individual's financial account
- Medical information
- Health insurance information
- Unique biometric data generated from measurements or technical analysis of human body characteristics, such as a fingerprint, retina, or iris image, used to authenticate a specific individual. Unique biometric data does not include a physical or digital photograph, unless used or stored for facial recognition purposes
- Genetic data
- Email addresses in combination with a password or security questions and answer that would permit access to the email.

**15. Do any of these laws require that I train my employees?**

With the exception of California, none of the consumer privacy laws expressly require that employees be trained. The CCPA, however, requires that covered businesses ensure that all individuals involved in implementing, managing, or overseeing compliance with the CCPA receive training. This includes executives, general managers, human resources employees, directors of marketing, social media managers, and information technology employees. Additionally, any employee responsible for handling consumer requests through the business's CCPA toll-free hotline must receive the training.

Even though most state consumer privacy laws don't require that you provide training, it is strongly recommended. You should train employees who regularly interface with consumers – such as sales representatives – on the basic requirements of the consumer privacy laws and where to direct consumer questions and requests regarding data privacy. Training raises awareness of the obligations of the business and can be used as a defense to any regulatory inquiry about the businesses' compliance. Fisher Phillips attorneys can provide training for employees on all aspects of consumer privacy laws and compliance.

***U.S. Privacy Hub***